Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1495

Vragen van het lid **Verhoeven** (D66) aan de Minister van Veiligheid en Justitie en de Minister-President over *het bericht dat de website van de rijksoverheid plat lag door een DDoS-aanval*. (ingezonden 17 februari 2015).

Antwoord van Minister **Blok** (Wonen en Rijksdienst) mede namens de Minister-President en de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie (ontvangen 9 maart 2015)

Vraag 1
Bent u bekend met de berichten «Ddos'ers wijzigden tijdens aanval rijksoverheid hun aanvalsmethode» en «rijksoverheid.nl was dupe van DDoS-aanval»?[1]

Antwoord 1
Ja.

Vraag 2
In 2013 heeft u een brief naar de Kamer gestuurd met een aantal maatregelen om de weerbaarheid tegen DDoS-aanvallen te vergroten; kunt u per punt aangeven wat de stand van zaken is ten aanzien van de implementatie?[2]

Antwoord 2
In de brief d.d. 14 mei 2013 en de eerdere brief over DDoS-aanvallen op de bancaire sector d.d. 16 april 2013 zijn de volgende acties aangekondigd:
1) Het nog dit jaar actualiseren van de Nationale Cyber Security Strategie;
2) Een geïntensiveerde aanpak van «Botnets» (netwerken van geïnfecteerde computers die gebruikt kunnen worden bij een (DDoS) aanval); en 3) Het aanpassen van het juridisch instrumentarium aan de ontwikkelingen in het digitale domein om middels gepaste opsporingsbevoegdheden cybercrime effectief te bestrijden. 4) Plaatsen filters bij DigiD en het preventief door de Minister van BZK afnemen van aanvullende diensten om grote aanvallen af te slaan. 5) De Minister voor Wonen en Rijksdienst en de Minister van Binnenlandse Zaken en Koninkrijksrelaties zullen samen met de Chief Information

[1] http://tweakers.net/nieuws/101329/ddosers-wijzigden-tijdens-aanval-rijksoverheid-hun-aanvalsmethode.html en http://nos.nl/artikel/2018594-rijksoverheid-nl-was-dupe-van-ddos-aanval.html

[2] http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/05/15/reactie-ddos-aanvallen-bij-de-rijksoverheid/lp-v-j-0000003271.pdf

ah-tk-20142015-1495
ISSN 0921 - 7398
's-Gravenhage 2015

Officers (CIO's) van de departementen, de medeoverheden, de interne en externe ICT dienstverleners en het NCSC verder bezien wat er nog voor aanvullende acties mogelijk zijn om de cyber security te verhogen en de impact van DDoS aanvallen op de belangrijke voorzieningen van de overheid te beperken. 6) De Minister van Algemene Zaken ziet toe op het op orde houden van de maatregelen tegen toekomstige DDos aanvallen van Rijksoverheid.nl. 7) Informatiedeling naar aanleiding van de ervaringen in 2013.

Hierbij per punt de stand van zaken:
1) In het najaar van 2013 is de Tweede Nationale Cyber Security Strategie gepubliceerd. Op 18 december 2014 is de eerste rapportage over de uitvoering hiervan aan de TK verzonden,
2) Naar aanleiding van het AO Cybersecurity d.d. 27 maart 2014 is de TK op 7 juli 2014 uitvoerig geïnformeerd over de geïntensiveerde aanpak van botnets. Een belangrijk onderdeel hiervan is de publiek-private samenwerking bij de bestrijding van botnets,
3) Over de versterking van het juridisch instrumentarium is in de eerdergenoemde rapportage d.d. 18 december aangegeven dat deze in de eerste helft van 2015 aan de Tweede Kamer zal worden aangeboden.
4) Naar aanleiding van de DDoS-aanvallen op DigiD in de periode van 23 april tot en met 27 april 2013 heeft Logius in opdracht van de Minister van Binnenlandse Zaken en Koninkrijksrelaties aanvullende maatregelen getroffen om uitval en/of verminderde beschikbaarheid te beperken en dergelijke aanvallen te kunnen mitigeren. Het gaat daarbij onder meer om het creëren van een grotere capaciteit in het verwerken van dataverkeer, en specifieke anti-DDoS tooling. Digitale voorzieningen van de overheid staan regelmatig bloot aan DDoS-aanvallen die variëren in aard en omvang. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen,
5) Om het bewustzijn ten aanzien van informatieveiligheid bij de medeoverheden te versterken, heeft de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) in twee jaar tijd vele activiteiten verricht. Een rapportage van de activiteiten is op 18 december 2014 naar de Tweede Kamer verstuurd (vergaderjaar 2014–2015, Kamerstuk 26 643, nr. 344). In het overleg van de CIO's van de departementen komt informatiebeveiliging regelmatig op de agenda.
6) Het Ministerie van Algemene Zaken ziet, geadviseerd door het NCSC, voortdurend samen met de leverancier toe of de genomen maatregelen nog toereikend zijn.
7) Het NCSC deelt beschikbare informatie over cyberaanvallen met de overheidsorganisaties om er lering uit te trekken en te bezien of (nieuwe) extra maatregelen moeten worden genomen. Dat gebeurt onder andere in zg. ISAC's (Information Sharing and Analysing Centres). In 2014 is de ISAC voor de overheid opgericht.

Vraag 3
Volgens het bericht «Ddos'ers wijzigden tijdens aanval rijksoverheid hun aanvalsmethode» werd een type DDoS-aanval gebruikt waar het hostingbedrijf geen ervaring mee had; kunt u aangeven of de maatregelen uit de brief van 2013 voldoende zijn om DDoS-aanvallen van dit type in voldoende mate te kunnen afslaan? Of zijn er nieuwe maatregelen nodig?

Antwoord 3
Bij elke soort DDoS aanval is het van belang om te werken met een combinatie van technische maatregelen, waaronder filtering en additionele capaciteit. De leverancier zal hiertoe een verbeterplan opstellen waarbij het Ministerie van Algemene Zaken en het NCSC nauw betrokken zijn. (zie ook de verklaring van de leverancier bij vraag 2 van Oosenbrug)
De maatregelen uit de brief van 2013 blijven in grote lijnen ook nu nog relevant, maar op technisch niveau zullen telkens weer nieuwe maatregelen moeten worden genomen.
Regelmatig vinden DDoS aanvallen plaats. In vrijwel alle gevallen worden deze met succes afgeslagen en blijft de aanval onopgemerkt voor het publiek. Daarnaast is het goed om te beseffen dat ondanks alle inspanningen er altijd een kans blijft op incidenten. Kwaadwillende personen vinden steeds weer

mogelijkheden om nieuwe en aanvullende beveiligingsmaatregelen te doorbreken. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen. Het gaat erom om tegen aanvaardbare kosten de risico's zo minimaal mogelijk te maken.

Vraag 4
Kunt u aangeven door wie en/of waarvandaan de DDoS-aanvallen zijn uitgevoerd?

Antwoord 4
Eventuele daders, motieven of achtergronden bij deze aanval zijn vooralsnog niet bekend. Het Ministerie van Algemene Zaken heeft aangifte gedaan

Vraag 5
Staat weerbaarheid tegen DDoS-aanvallen op de agenda van de conferentie over cybersecurity in april 2015 in Nederland? Zo nee, bent u bereid het op de agenda te zetten?

Antwoord 5
Nee, het specifieke onderwerp DDoS-aanvallen staat niet als dusdanig op de agenda. Wel komen maatregelen zoals normen en standaarden die bijdragen aan de weerbaarheid tegen dergelijke aanvallen prominent voor op de agenda. Over de nadere inhoud van de conferentie zal de Kamer nog deze maand geïnformeerd worden.

Vraag 6
Waarom is ervoor gekozen geen tijdelijke noodwebsite te plaatsen waarmee mensen verwezen kunnen worden naar andere informatiekanalen?

Antwoord 6
Die keuze is een afweging tussen kosten en baten en de tijd, die nodig is om een omvangrijke site als rijksoverheid.nl elders op een veilige wijze in de lucht te krijgen. Gezien de kosten en de benodigde tijd is deze keuze niet gemaakt.
Voor de getroffen sites bestaat een back-upvoorziening, die echter ook getroffen bleek. De leverancier zal een verbeterplan opstellen waarbij het Ministerie van Algemene Zaken en het NCSC nauw betrokken zijn. Onderdeel van dat plan zal zijn te regelen, dat deze back-up voorziening bij een DDoS aanval wel kan worden ingeschakeld.

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van het lid Dijkhoff (VVD), ingezonden 13 februari 2015 (vraagnummer 2015Z02658)